REMARKS/ARGUMENTS:

Claims 26-41 are pending in this application. Claims 1-25 have been canceled by way of this amendment without prejudice or disclaimer to the subject matter contained therein. New pending claims 26-41 have been added by way of this amendment.

General Remarks

The present invention provides a versatile integrated access device, and a distributed subscriber management system using the same. The integrated access device interfaces with several user networks and with an access network, which connects the user networks to "external networks" (in general to network servers). The intent is to perform several management functions – primarily authentication/authorization – locally, for requests sent by users located within the user networks to access the external networks, avoiding the need to traverse the access network for most of the control-data traffic.

Applicant submits that the claimed system and access device are not anticipated in the prior art. The Examiner cites the following references:

(1) U.S. Patent Number 6,463,474 to Fuh *et al.* (hereinafter "Fuh");
(2) U.S. Patent 6,584,505 to Howard *et al.* (hereinafter "Howard");
(3) U.S. Patent 5,491,752 to Kaufman *et al.* (hereinafter "Kaufman");
(4) U.S. Patent 5,546,387 to Larsson *et al.* (hereinafter "Larson");
(5) U.S. Patent 6,377,955 to Hartmann et al. (hereinafter "Hartman");
(6) Patent 5,903,564 to Ganmukhi *et al.* (hereinafter Ganmukhi");
(7) U.S. Patent 6,311,275 to Jin *et al.* (hereinafter "Jin");
(8) U.S. Patent 6,466,977 to Sitaraman et al. (hereinafter "Sitaraman"); and
(9) U.S. patent 6,510,454 to Walukiewicz (herein after "Walukiewicz").

The Fuh reference

An exemplary environment in which the Fuh invention is utilized is depicted in Figures 2 and 3 in Fuh. Fuh discloses a computer system for controlling access of a client to a network resource using a network firewall routing device. Fuh considers a local area network 206 and a single target server and discloses a method of controlling access of a client located in the local area network to the network resource.

On page 3, paragraph 5 of the office action, the Examiner states that "Fuh discloses receiving, at an access control node/authentication proxy, which is operatively coupled to a plurality of user networks (FIG. 4)".

Applicant respectfully points out that FIG. 4 in Fuh illustrates a single user 302 (a personal computer for example) residing in a LAN 206. Fuh does not contemplate multiple LANs sharing an access control device. Figures 2, 3, and 4 in Fuh refer to the same environment. Please see the passages below:

Col. 8, lines 9-13: "FIG. 2 is a block diagram of a system 200 in which an embodiment of an Authentication Proxy can be used. Generally, system 200 includes a LAN 206, and a local, packet-switched network that uses Internet protocols, or intranet, 216."

Col. 8, lines 49-52: "FIG. 3 is a block diagram showing certain internal details of the system in FIG. 2. In this example, one of the network devices 208a-208c of LAN 206 is a client 306, such as a personal computer or workstation."

Col. 9, lines 6-7: "As in FIG. 3, the system of FIG. 4 includes User 302 who is associated with Client 306. A Browser 304 is executed by Client 306, which is part of LAN 206."

Applicant respectfully submits that the Fuh reference lacks the differentiating feature of the present invention, which is to provide concentration of authorization traffic (and optionally other control traffic) generated within multiple user networks to share a common authentication/authorization device.

The Howard reference

An exemplary network environment in which the Howard invention is utilized is depicted in FIG. 1 of the Howard reference. A client computer system 100, an authentication server 110, and web servers 104, 106, and 108 are interconnected through a network 102 (the Internet, for example). In general, the authentication server 110 may be shared by numerous client computer systems 100 which may access many web servers. The Howard system permits authentication-resource sharing throughout the network. However, it requires that data needed to complete each authentication/authorization process cross the network 102 (please see col. 3, lines 44-51 in Howard). Thus, Howard teaches away from the system of the present invention. In contrast, the main objective of the present invention is to eliminate, or significantly reduce, such exchange through the network 102.

The Kaufmann reference

Kaufman discloses an improved security system to render password guessing difficult and to inhibit eavesdropping, dictionary attacks, and intrusion into stored password lists.

The Larsson reference

The Larsson reference is concerned with label processing at incoming and outgoing links of a packet switch. The invention provides a network and a packet switch adapted to efficiently handle label processing at the incoming and outgoing sides of a switch. The Larson invention does not consider any issue related to access security or user authentication.

The Hartmann reference

Hartmann discloses a method and apparatus for dynamically generating a network performance report based on RADIUS network accounting information.

The Ganmukhi reference

Ganmukhi discloses a technique of efficient internal routing within an ATM switch with multicast capability.

The Jin reference

Jin discloses a method for providing single step log-on access for a subscriber to a computer network that comprises public and private areas. Secure access to the private areas is provided by a Service Selection Gateway Server.

The Sitaraman reference

Sitaraman discloses a system for dynamically identifying a preferred one of a plurality of AAA services at a remote domain to which an access request is routed.

The Walukiewicz reference

Walukiewicz discloses a device comprising monitoring circuitry configured to monitor a communications link to detect an alarm condition.

Applicant respectfully submits that none of the above references provides all the features of the present invention as defined in claims 26-41. Furthermore, no combination of the above references leads to all the features of independent claims 26, 32, and 38.

Claim Rejections – 35 USC 102

In the outstanding office action, **claims 1, 3, 12, 15, and 25** are rejected under 35 U.S.C. 102(e) as being anticipated by Fuh.

Claims 1-12 and 14-25 have been canceled by way of this amendment without

prejudice. However, some of the features claimed therein are reintroduced in the new set of claims. As discussed above, the Fuh reference is missing the feature of providing a common authentication/authorization device to be shared by multiple user networks, which characterizes the present invention.

Claims 1, 15, and 25 are rejected under 35 U.S.C. 102(e) as being anticipated by Howard.

Claims 1, 15, and 25 have been canceled by way of this amendment without prejudice. However, some of the features claimed therein are reintroduced in the new set of claims. As discussed above, Applicant respectfully points out that while the Howard scheme provides a common authentication server 110 (FIG. 1 in Howard) to be shared by multiple users, it requires that the authentication traffic traverse the access network 102 to reach the common server and "affiliate servers". The authentication server 110 in Howard is also a web server capable of interacting with other web servers. The Howard scheme misses some major advantages of the present invention: (1) The scheme permits unauthorized traffic to cross the access network 102, hence wasting network resources (both in terms of transport and processing) while the present invention avoids such waste, (2) The common server 110 does not lend itself to flow-rate control (often called "bandwidth allocation and enforcing") while the integrated access device of the resent invention performs this function handily, being placed in logical and physical proximity to the multiplicity of user networks it serves, (3) The common server 110 cannot provide encryption of access control information, which is one of capabilities of the integrated access device of the present invention, and (4) The common server 110 has no control over direct communications between user networks while the integrated access device provides this function to the set of user networks it serves.

As such, Applicant submits that the Howard reference does not provide the essential feature of the present invention of directly connecting a plurality of user networks to a common versatile integrated access device. Furthermore, it is noteworthy that the Fuh scheme and the Howard scheme are mutually exclusive; the former being based on pre-switching conditions while the latter is conditioned for post-switching limitations.

Claim Rejections – 35 USC 103

Claims 2, 6, 7, 11, 17, and 20 are rejected under 103(a) as being unpatentable over Fuh, in view of Howard.

Claims 2, 6, 7, 11, 17, and 20 have been canceled without prejudice. Their content has not been reintroduced in the new set of claims.

Claim 5 is rejected under 35 USC 103(a) as being unpatentable over Fuh in view of Howard, and further in view of U.S. patent 5,491,752 to Kaufman et al.

Claim 5 has been cancelled by way of this amendment.

Claims 8, 9, and 24 are rejected under 35 USC 103(a) as being unpatentable over Fuh, in view of Howard, and further in view of Metz.

Claims 8, 9, and 24 have been canceled. Their content has not been reintroduced in the new set of claims.

Claim 10 is rejected under 35 USC 103(a) as being unpatentable over Fuh, in view of Larsson. Claim 10 has been canceled but its content is partially reintroduced as claim 28.

Applicant respectfully points out that Larsson describes conventional data labeling, a process which is essential for enabling routing data units through a network while the data unit labeling scheme of the present invention is intended to add a security measure. As described in paragraphs 47 and 58 of the published application 20010044893 of the present invention, the secure data labeling scheme renders a data unit illegible to an unintended device while in transit across the access network.

New claim 28 depends from new claim 26 which claims a system comprising a plurality of user networks connected to an integrated access device. As discussed above, the Fuh reference does not address multiple user networks sharing a control device, and the Larsson reference does not consider secure data labeling, and it is respectfully submitted that the combination of Fuh and Larsson does not lead to claim 28.

Claim 14 is rejected under 35 USC 103(a) as being unpatentable over Fuh in view of Hartmann. Claim 14 has been canceled by way of this amendment.

Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Fuh in view Ganmukhi. The claimed matter has been reintroduced in new claim 37.

Applicant respectively points out that claim 16 relates to an integrated access device which does not exist in Fuh. The claim further characterizes the integrated access device as

having multiple ingress cards, indicating that the device supports a plurality of user networks. A person skilled in the art knows that any switching unit/device, regardless of its mode of operation, has a plurality of ingress ports and a plurality of egress ports which are typically paired into dual ports and packaged in at least one card. The Ganmukhi reference, which is concerned with mapping multi-cast identifiers onto local identifiers in an ATM switch, mentions in passing in its opening paragraph of the background section (col. 1, lines 13-29) that the ATM switch under consideration has ingress cards and egress cards.

Applicant submits that the combination of Fuh and Ganmukhi does not lead to claim 37. Furthermore, it is submitted that motivation to combine Fuh and Ganmukhi to arrive at claim 37 is found neither in Fuh nor in Ganmukhi. This is expected because Fuh has no use for an integrated access device, and Ganmukhi is primarily concerned with multicasting.

Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Fuh in view of Jin. Claim 18 has been canceled; its content has not been introduced in the new claims.

Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Fuh, in further view of Sitaraman, Hartmann, and Walukiewicz. Claim 19 has been canceled, but its content has been reintroduced in claim 34.

With respect to the Sitaraman reference, Applicant respectfully points out that the passage in Sitaraman, col. 3, lines 14-41, refers to a process of selecting from among a plurality of AAA servers. The Sitaraman invention is summarized in col. 3, lines 30-41 to comprise two main processes:

(1) "A Wholesaler dynamically identifies one of a plurality of AAA services at a remote domain to route an access request to"; and

(2) "A Wholesaler, based upon a Service Level Agreement (SLA) between the Wholesaler and a user, routes the user to one of a plurality of sub-service providers."

In contrast, in the distributed subscriber management system of the present invention, the user network interface of the integrated access device, which may accommodate several user networks, is designed to offer different levels of bandwidth availability to the different user networks (please see paragraph 55 of USPTO publication 2001-0044893). The system allows providers to sell services based on guaranteed bit rates by allocating discrete bandwidth levels to individual user networks and enforcing the bandwidth through bandwidth management techniques. No such feature is contemplated in Sitaraman.

With respect to the Hartmann reference, Col. 1, lines 34-56, in the background section, describes a conventional process of collecting usage data. Applicant notes that such a process has been extensively used in commercial telecommunication networks for several decades. Claim 34 of the present invention associates "means for statistical usage collection" with a novel integrated access device, thus further increasing the functional diversity of the claimed integrated access device.

With respect to the Walukiewicz reference, detecting and reporting alarm conditions in telecommunication networks are rudimentary processes which have been implemented in numerous forms. The Walukiewicz reference describes a network device which monitors a communications link in a network, detects an alarm condition relevant to the monitored link, and sends an electronic-mail message to a recipient device for action. Col. 1, lines 19-33, in the background section in Walukiewicz emphasizes the need for alarm systems in a general computer network.

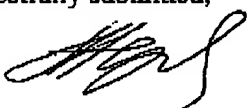
Applicant notes that the device of Walukiewicz is link-specific. In contrast, claim 34 of the present disclosure teaches optional incorporation of means for alarm monitoring in the novel integrated access device, thus adding a useful limitation to a claim base believed to be allowable. It is submitted that all the elements claimed in claim 34 are not found in the combination of Fuh, Sitaraman, Hartmann, and Walukiewicz.

Conclusion

Claims 1-12 and 14-25 have been canceled by way of this amendment without prejudice or disclaimer to the subject matter contained therein. Claims 26-41 have been added by way of this amendment. No new material has been added.

Favorable consideration and allowance of claims 26-41 of the application is earnestly solicited.

Respectfully submitted,



Victoria Donnelly, Registration No. 44,185
Tropic Networks Incorporated
Intellectual Property Department
135 Michael Cowpland Drive,
Kanata Ontario, Canada K2M 2E9
Telephone: (613) 270-6026
Facsimile: (613) 270-9663